529213

Rec'd PCT/PTO 25 MAR 2005

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 avril 2004 (08.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/030394 A1

(51) Classification internationale des brevets[7] : H04Q 7/38, H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR2003/002837

(22) Date de dépôt international :
26 septembre 2003 (26.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/11944 26 septembre 2002 (26.09.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : GEMPLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activité de Gémenos, F-13420 Gemenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : DE GROOT, Max [NL/FR]; 10, LOT. L'Acadie, F-13720 La Bouilladisse (FR).

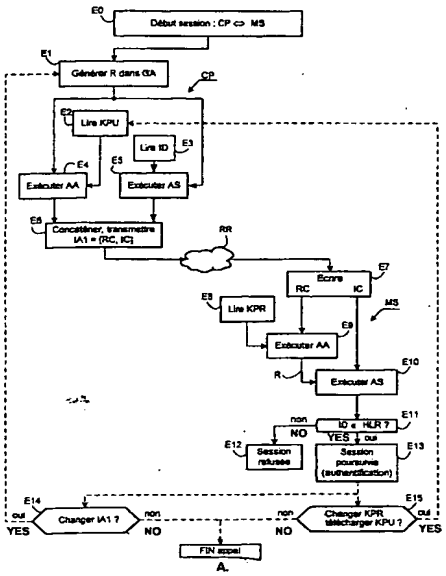
(74) Mandataire : NONNENMACHER, Bernard; Gemplus / La Vigie, Zone Athélia IV, Avenue du Jujubier, BP 90, F-13705 La Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: IDENTIFICATION OF A TERMINAL WITH A SERVER .

(54) Titre : IDENTIFICATION D'UN TERMINAL AUPRES D'UN SERVEUR



E0...STARTING SESSION
E1...GENERATING RANDOM NUMBER
E2...READING KPU
E3...READING ID
E4...EXECUTING AA
E5...EXECUTING AS
E6...CONCATENATING, TRANSMITTING IA1 = (RC. IC)
E7...READING RC, IC
E8...READING KPR
E9...EXECUTING AA
E10...EXECUTING AS
E11...ID ∈ HLR ?
E12...NO, SESSION DENIED
E13...YES, SESSION MAINTAINED (AUTHENTICATION)
E14...MODIFY IA1 ?
E15...MODIFY KPR OR DOWNLOAD KPU ?
A...END

(57) **Abstract:** A chip card (CP) in a terminal such as a mobile radiotelephone identified by a first identifier (ID) with a server (MS) including for example the nominal locating recorder in a cellular radiotelephone network, without the first identifier being transmitted in clear or substituted by a provisional identifier. An anonymous identifier (IA1) is determined in the card on the basis of a generated random number (R), of the first identifier (ID) and on the result of a public key (KPU) asymmetric algorithm (AA) whereto at least the random number is applied. The anonymous identifier is transmitted to the server which recovers the first identifier at least by executing the asymmetric algorithm to which a private key (KPR) and at least partly the anonymous identifier are applied.

(57) **Abrégé :** Une carte à puce (CP) dans un terminal tel que radiotéléphone mobile est identifiée par un premier identificateur (ID) auprès d'un serveur (MS) incluant par exemple l'enregistreur de localisation nominal dans un réseau de radiotéléphonie cellulaire, sans que le premier identificateur soit transmis en clair ou remplacé par un identificateur provisoire. Un identificateur anonyme (IA1) est déterminé dans la carte en fonction d'un nombre aléatoire généré (R), du premier identificateur (ID) et du résultat d'un algorithme asymétrique (AA) à clé publique (KPU) auquel au moins le nombre aléatoire est appliqué. L'identificateur anonyme est transmis au serveur qui récupère le premier identificateur au moins par exécution de l'algorithme asymétrique auquel une clé privée (KPR) et au moins partiellement l'identificateur anonyme sont appliqués.

WO 2004/030394 A1

Rec'd PCT/PTO 28 FEB 2005

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.